State of Colorado
Cyber Security Policies

System and Applications Security Operations

Overview

This policy document is part of the State of Colorado Cyber Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). All Agencies within the scope of this Policy must support and comply with the Requirements section of this document. Additional best-practice guidance is outlined in the Guidelines Section which has been designed to help an Agency achieve the objective of this Policy.

For the purposes of this document, an “Agency” includes organizations as defined in C.R.S. 24-37.5-102(5).

Authority

C.R.S. 24-37.5-401(1), C.R.S. 24-37.5-403(2)(b)-(c), C.R.S. 24-37.5-404(2)(b).

Scope

This policy document applies to every State agency ("Agency") as defined in C.R.S. 24-37.5-102(5). "State agency" means every state office, whether legislative, executive, or judicial, and all of its respective officers, departments, divisions, commissions, boards, bureaus, and institutions. "State agency" does not include State-supported institutions of higher education, the department of higher education, the Colorado commission on higher education, or other instrumentality thereof.

Policy

Agencies shall protect information assets, data and reputation while providing a secure framework for System and Applications Operations. All agencies shall implement technical controls identified in the Agency Cyber Security Plan and justified by the Agency Risk Assessment in accordance with the Colorado Cyber Security Program.

Definitions

For the purposes of this document, refer to C.R.S. 24-37.5-102, C.R.S 24-37.5-402, and the Colorado Cyber Security Program Policy Glossary for any terms not specifically defined herein.

Roles and Responsibilities

Executive Director – responsible for:

- Ensuring adequate budget is allocated to the IT staff to support the required controls in this policy.
- Ensuring training initiatives that support the introduction of new technology are funded appropriately.

Agency Chief Information Officer (CIO) – is responsible for:

- Ensuring the Agency Cyber Security Plan appropriately addresses the controls in this policy.
- Ensuring the functions supporting these controls are sufficiently budgeted for and includes all labor and capital expenditures.
- Reviewing the deliverables of these controls and using the outputs to drive an Agency improvement process.
- Ensuring administrator training is accounted for when introducing new technology into the environment.

Agency Information Security Officer (ISO) – is responsible for monitoring technical safeguards and systems security controls.

IT Staff – **is** responsible for deploying technical safeguards and systems security controls.

Requirements

The Agency CIO, in conjunction with the Agency Information Security Officer, shall define, maintain and enforce written procedures for systems network operations that include the inventories, processes and procedures for the following activities:

Access Controls

In accordance with Access Control Policy, P-CCSP-008, all Agencies shall ensure unique user ids, proper password usage and monitoring of user login attempts.

At a minimum, procedures are to be implemented to enforce the following systems access controls:

- **User Identification**
  The Agency ensures all systems require and implement unique user names for authentication.
- **Logical Access Controls**
  - Password Management is to be followed according to the password section of the CCSP Access Control Policy, P-CCSP-008.
  - Systems are set to automatically log off users or enable session-locking mechanisms after a maximum of 15 minutes of inactivity.

- Accounts are locked out for a period of time after three failed log-in attempts. For Administrator accounts, System Administrator reset procedures are required to enable locked accounts.

- Agency-level policy and procedures dictate standards for granting systems access at a level commensurate with job responsibilities assigned to each user and the principle of least privilege in accordance with the CCSP Access Control Policy, P-CCSP-008.

- All Agencies are to implement password management in accordance with the Access Control Policy, P-CCSP-008.

- Agencies are to ensure system individual administration credentials (e.g., username and password, token and pass phrase) are not shared.

- Agencies are to ensure that remote system administration sessions (e.g., telnet or http connections for administrative purposes) are encrypted (e.g. SSH or SSL).

- **Physical Access Controls**
  The Agency shall maintain physical access controls according to the CCSP Access Control Policy, P-CCSP-008 and CCSP Physical Security Policy, P-CCSP-010.

- **Log-in Monitoring**
  Log-in monitoring shall be conducted according to procedures supporting the monitoring section of the CCSP Access Control Policy, P-CCSP-008.

- **Log-On Banner and Security Reminders**
  Each Agency shall enforce the use of Log-On banners to remind each State system user of his/her responsibilities while accessing State systems. Specific verbiage is not provided here, but the log-on banner must contain the following:
  - Use is being monitored; users have no expectation of privacy
  - Use of the system confirms acceptance of the Agency Cyber Security Plan and sanctions for non-compliance
  - Attempts to defeat security mechanisms are treated as a security incident and are potentially subject to civil and/or criminal penalties.
  - Use of the system confirms acceptance of the System Access and Acceptable Use Policy, P-CCSP-013.

System Administration and Engineering

System Administration and Engineering activities shall be optimized to protect sensitive information in addition to providing a platform to meet the Agency's functional and operational requirements. At a minimum, each Agency defines and publishes procedures, diagrams, and inventories to accomplish the following:

- **Inventory and Maintenance Records**
  - Inventory critical systems, applications, and any specific proprietary system information and maintain this inventory for Disaster Recovery purposes in accordance with the Change Control Policy, P-CCSP-009.

- Agencies are to keep its inventory current and make it available to the Colorado Cyber Security Incident Response Team (CSIRT).
- Agencies are to notify the Information Security Operations Center (ISOC) when inventories are updated and share the updated information with the ISOC.

- **Perimeter Security**
  Each Agency deploys and maintains perimeter security protection in accordance with the Network Operations Policy, P-CCSP-006, which includes:
  - All Agency public-facing systems must be deployed in a DMZ that controls both ingress and egress from both internal and external networks.
- **Back-up and Recovery**
  The Agency CIO shall establish data back-up procedures to recover information according to recovery objectives established in the Agency Disaster Recovery Plans and in accordance with the Disaster Recovery Policy, P-CCSP-004.
- **Encryption**
  - The Agency CIO shall deploy encryption controls for sensitive information in transmission and during storage on State systems as justified by the State risk assessment and the Data Handling and Disposal Policy, P-CCSP-011.
- **Training**
  - All Agencies shall ensure that system administrators are sufficiently trained and skilled to perform their duties.

Change Control and Configuration Management

In accordance with Change Control Policy, P-CCSP-009, all Agencies are to ensure changes to systems are approved in a controlled manner and the system configuration information is consistent with an approved baseline.

Servers, workstations, network devices and security systems hardening are implemented according to standards approved by each Agency and identified in the Agency Cyber Security Plan. At a minimum:

- Document the purpose of each system with the minimum server and software required for proper system operation.
- Install minimum hardware and software to accomplish the specific purpose and disable non-essential services.
- Establish standards consistent with best practices recommend by vendors and industry sources such as the National Institute for Standards and Technology (NIST) or the National Security Agency (NSA).
- Enable logging on all systems in accordance with Agency Standards and in compliance with the Colorado Cyber Security Plan (CCSP) Security Metrics and Measurement Policy P-CCSP-017.
- Remove all guest accounts and default passwords.
- Test all system configurations prior to deployment.

Patch Management

All Agencies shall ensure operating systems and application software is kept current with vendor-issued security patches.

Each Agency shall establish procedures to monitor vulnerability warnings from manufacturers, regulators, industry sources, and the Information Security Operations Center (ISOC). Response to ISOC vulnerability warnings is made to the ISOC within 72 hours with a description of the planned mitigation activities and the time frames in which they are to occur.

Agencies are to routinely scan all critical and general support systems for vulnerabilities and missing patches.

Agencies are to describe the acceptable windows for applying patches according to their criticality as published by the Vendor in their Agency Cyber Security Plan (ACSP).

Malicious Code

All agencies shall establish procedures and controls that meet the following objectives:

- **Malicious Software Protection**
  Each Agency describes its Malicious Code protection controls in the ACSP. At a minimum, it includes:
  - Deploying virus protection software on all Agency workstations and at the e-mail gateway
  - Configuring virus protection software to perform a full scan at least weekly.

Monitoring and Reporting

All Agencies shall, at a minimum, monitor anomalous system activity. All suspicious activities are to be reported to the Agency ISO and handled as a Security Event in accordance with the Incident Response Policy, P-CCSP-002.

- **System Logging**
  Logging is enabled for each critical system in accordance with the Access Control Policy, P-CCSP-008.
  - System and Application Logs for critical systems are maintained for a period of at least one year for forensics purposes as part of the Cyber Security Incident Response Plan (CSIRP). See the CSIRP for forensic log retention requirements.

System Backups

All Agencies shall perform system backups in accordance with business continuity needs and the Disaster Recovery Policy P-CCSP-004.

Backups are to be stored in a separate facility than the Agency IT resources which they back up and in secure containers consistent with the Data Handling and Disposal Policy, P-CCSP-011.

Guidelines

This section describes best practices for meeting the objective of this policy.

Access Controls

New systems and applications shall be written to leverage two-factor authentication where applicable.

System Administration and Engineering

- **Perimeter Security**
  - Separate all user Local Area Network (LAN) segments from production servers through the use of a firewall or Access Control Lists.
- **Malicious Software Protection**
  - Update virus protection software and virus signatures on a daily basis.
- **Vulnerability Assessment and Patch Management**
  - Test systems prior to deploying patches or vulnerability work-arounds in a production environment.
- **Host system redundancy**
  - Ensure all Systems and Applications with High Availability requirements have redundancy mechanisms to minimize the probability of downtime.
- **Back-up and Recovery**
  - Label as confidential all back-up media containing sensitive information.
- **Encryption**
  - If the Agency maintains encryption services (to include key generation, backup, escrow, or recovery) to the Agency user community or to external entities, the Agency CIO deploys encryption key management procedures governing such services.
- **File Integrity Management and Host-Based IDS**
  - The Agency CIO deploys file integrity monitoring and/or Host IDS to alert operations staff to unauthorized modification of critical systems or content files stored on those critical systems that contain sensitive information.

Change Control and Configuration Management

- **Configuration Management**
  - Verify the most current version of hardware and software is installed.
  - Configure privileges by first denying all access and then allowing the minimum access to each user.
  - Encrypt all encryption private key files.

- Test all systems though an independent administrator prior to deploying the system in a production environment.

Patch Management

- Patching is coordinated with the backup schedule to ensure that systems can be recovered in the event of system disruption due to a patch.
- Master configuration lists are updated to note what patches have been installed after each patch has been deployed.
- Patches rated as "critical" are applied within five working days; "high" patches are applied within ten working days; "medium" rated patches are applied within thirty working days; and "low" rated patches are applied as needed. The Agency ISO is responsible for the final determination of the patch rating, but defers to the Information Security Operations Center (ISOC) and the State CISO's office when a rating is available from either entity.
- Exceptions may be granted with justification (e.g., application incompatibility) by the Agency CIO with the stipulation that mitigation of the condition causing the exception is documented in the Agency's Plan of Action and Milestones (see the Cyber Security Planning Policy P-CCSP-001 for details).

Malicious Code

All systems, including Workstations and Servers, must anti-virus software installed and configured to perform a comprehensive scan at least weekly.

All virus signatures on all systems is updated daily.

Agencies are to deploy anti-spam at the e-mail gateway and anti-spyware controls on all systems.

Agencies keep the anti-virus software "engine" within one revision of the most current.

Agencies keep the anti-virus "signature" data updated to the most current version.

Monitoring and Reporting

Each Agency shall establish procedures for the following tasks:

- **Central Event Log Analysis**
  - Event logging is to be consolidated to facilitate trend analysis and security monitoring.
  - Automated Alert notification are to be enabled to accelerate response to failures and policy violations identified in the logs.
  - Event logs to include both system logs and access control logs are to be maintained for a period of at least six months to document forensic evidence in case system abuse is investigated.
- **Network Capacity, Performance and Fault Monitoring**
  Deploy network capacity, performance and fault monitoring to aid in the management and recovery of systems and well as conduct forensic investigations in the event problems or complaints are investigated.

References

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64 "Security Considerations in the Information System Development Life Cycle"
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 "Recommended Security Controls for Federal Information Systems"
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-40 Version 2 "Creating a Patch and Vulnerability Management Program"